Strategy Research Project

U.S. Cybersecurity Defense Assessment

by

Commander Darren C. Sherman
United States Navy

United States Army War College
Class of 2013

REPORT DOCUMENTATION PAGE	Form Approved OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
xx-03-2013	STRATEGY RESEARCH PROJECT	

4. TITLE AND SUBTITLE
U.S. Cybersecurity Defense Assessment

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Commander Darren C. Sherman
United States Navy

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Dr. Adam Silverman
Department of National Security & Strategy

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army War College
122 Forbes Avenue
Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution A: Approved for Public Release. Distribution is Unlimited.

13. SUPPLEMENTARY NOTES
Word Count: 6,417

14. ABSTRACT

In today's global cybersecurity environment, U.S. federal agencies and private sector organizations are engaged in national cyber defense actions designed to protect against intrusion from state and non-state actors, foreign militaries, organized crime, and sophisticated hackers attempting to commit malicious activity or espionage against America's essential networks. The purpose of this paper, which concentrates in US cybersecurity defense as a strategic "way" of supporting America's enduring national security interests, is threefold. To define cybersecurity defense in a paradigm that is universally acceptable within the American construct; to identify and discuss U.S. cybersecurity defense strategies by examining the progression of America's cybersecurity defense policies and the subsequent Federal agency roles which have developed within the U.S. government configuration; and provides a recommendation to improve America's national cybersecurity defense posture by implementing public-private partnership information sharing programs for critical network infrastructure security within the Defense Industrial Base (DIB) sector.

15. SUBJECT TERMS
Cyber Security Defense

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPHONE NUMBER *(Include area code)*
UU	UU	UU	UU	38	

USAWC STRATEGY RESEARCH PROJECT

U.S. Cybersecurity Defense Assessment

by

Commander Darren C. Sherman
United States Navy

Dr. Adam Silverman
Department of National Security & Strategy
Project Adviser

This manuscript is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Abstract

Title:	U.S. Cybersecurity Defense Assessment
Report Date:	March 2013
Page Count:	38
Word Count:	6,417
Key Terms:	Cyber Security Defense
Classification:	Unclassified

In today's global cybersecurity environment, U.S. federal agencies and private sector organizations are engaged in national cyber defense actions designed to protect against intrusion from state and non-state actors, foreign militaries, organized crime, and sophisticated hackers attempting to commit malicious activity or espionage against America's essential networks. The purpose of this paper, which concentrates in US cybersecurity defense as a strategic "way" of supporting America's enduring national security interests, is threefold. To define cybersecurity defense in a paradigm that is universally acceptable within the American construct; to identify and discuss U.S. cybersecurity defense strategies by examining the progression of America's cybersecurity defense policies and the subsequent Federal agency roles which have developed within the U.S. government configuration; and provides a recommendation to improve America's national cybersecurity defense posture by implementing public-private partnership information sharing programs for critical network infrastructure security within the Defense Industrial Base (DIB) sector.

U.S. Cybersecurity Defense Assessment

> To establish a front line of defense against today's immediate threats by creating shared situational awareness of network vulnerabilities, threats, and events within the Federal Government… and private sector partners… to act quickly to reduce… vulnerabilities and prevent intrusions.
>
> —2008 Comprehensive National Cybersecurity Initiative

The digital information and communications infrastructure referred to as "cyberspace" supports almost every facet of modern society and provides essential services for the United States economy, its critical infrastructure, and national defense. However, technology that is used to connect American global networks in ways never before previously envisioned is a mounting problem for the Federal government. This quandary exist because the nation's computer networks are routinely plagued by cyber intrusions from foreign and domestic adversaries seeking illicit access to sensitive public and private information. Moreover, technically proficient cyberspace intruders are using electronic incursions as a vehicle to weaken the U.S. economy and degrade U.S. national security, by stealing billions of dollars[1] worth of intellectual property and classified government secrets. For example, as more Americans in private business and government agencies increase their access to and use of cyberspace, the problem of cybersecurity is escalating and without adequate solutions, this issue will quickly become a serious 21st Century challenge to U.S. National Security.

In 2009, President Obama confirmed cybersecurity defense as a significant national security interest that the U.S. government [was] not adequately prepared to counter.[2] In actuality, it appears that cyberspace technology intended to foster national security and enhance the U.S. economy is in fact leveraging cyber related safety in the opposite direction.[3] As a result, the realm of cyberspace and the associated safety

measures implemented to police and safeguard it, has created a unique American cybersecurity defense issue for the Federal government– "the dual challenge of maintaining an environment that promotes efficiency, innovation, economic prosperity, and free trade while also promoting safety, security, civil liberties, and privacy rights."[4]

The purpose of this paper, which concentrates in US cybersecurity defense as a strategic "way" of supporting America's enduring national security interests, is threefold. First, I will define cybersecurity defense in a paradigm that is universally acceptable within the American construct. I will then identify and discuss U.S. cybersecurity defense strategies by examining the progression of America's cybersecurity defense policies and the subsequent Federal agency roles that have developed within the U.S. government configuration. Finally, I will provide a recommendation to improve America's national cybersecurity defense posture by assessing two recently endorsed U.S. cybersecurity defense initiatives: implementation of the public-private partnership information sharing program that facilitates improvement of critical network infrastructure within the Defense Industrial Base (DIB) sector; and the strategic importance of Cybersecurity Defense Act (2012) legislation, as it applies to national and federal network security protection. In today's global cybersecurity environment, U.S. federal agencies and private sector organizations are engaged in national cyber defense actions designed to protect against intrusion from state and non-state actors, foreign militaries, organized crime, and sophisticated hackers attempting to commit malicious activity or espionage against America's essential networks.

In order to effectively apply national cybersecurity defense measures against these cyberspace attacks, the term cybersecurity defense must be clearly defined. For

example, at each level of government – political, strategic, operational, and tactical, differing points of view exist regarding strategic level cybersecurity defense.[5] These varying perspectives influence how cybersecurity defense is defined and how national cybersecurity strategy is interpreted and implemented. Moreover, the terms national cybersecurity and cybersecurity defense are used synonymously in U.S. policy discussions, which further complicates classifying cybersecurity defense. This is an important distinction because different definitions of cybersecurity have significant implications on the actions or operations of cybersecurity defense agencies and impacts the cybersecurity defense roles adopted by various levels of government during national policy and strategy formulation.

Analyses of twenty different cybersecurity strategies in the North Atlantic Treaty Organization's (NATO) National Cyber Security Framework Manual[6] reveal that diverging variations of cybersecurity defense definitions are common. This manual advocates that government organizations differentiate their cybersecurity defenses activities based upon national cybersecurity perspective, unique network capabilities, and or Federal agency partnerships.[7] For example, several cybersecurity strategies contained in this manual[8] propose the integration of multi-dimensional cyber security efforts in which government, society, and influential stakeholders work together in cooperation to provide adequate levels of cybersecurity defense.[9] Exacerbating this situation, many of the cybersecurity defense processes developed to support cybersecurity definitions hinder generic government collaboration internally. However, to what end is not so clearly identified and different cybersecurity strategies are based uniquely upon different cybersecurity definitions. Within the complex conceptual

framework of cybersecurity defense, the United States has established the following three definitions used interchangeably throughout the cybersecurity defense strategy formulation process.

One cybersecurity defense paradigm embraced by the U.S. Department of Defense (DOD) is characterized as organizational actions required to ensure "security of information in all its forms – electronic and physical, and the security of the systems and networks where information is stored, accessed, processed, and transmitted, including precautions taken to guard against crime, attack, sabotage, espionage, accidents and failures."[10] This definition is especially useful for DoD operations, as it does not limit the departments' actions in mitigating potential cyber threats. Another cybersecurity defense classification is utilized by the U.S. military services and integrates a Joint Operations point of view. This definition advocates the use of Computer Network Defense (CND) actions to include "protecting, monitoring, analyzing, detecting, and responding to unauthorized activity within Department of Defense (DoD) information systems and computer networks."[11] Again the premise behind this classification is freedom to maneuver regarding cybersecurity defensive actions. Lastly, U.S. Cyber Command (USCYBERCOM) uses a strictly operational taxonomy to describe cybersecurity defensive operations – "direct and synchronized actions to detect, analyze, counter and mitigate cyber threats and vulnerabilities; to out maneuver adversaries taking or about to take offensive actions; and to otherwise protect critical missions that enable US freedom of action in cyberspace."[12] While all of the actions contained in these definitions are fundamental to the successful defense of critical

national and federal network systems, the USCYBERCOM explanation is the most directive in implying a position of offensive action.

In order to better understand how the U.S. translates these definitions into strategic action a sequential review of the six primary national cybersecurity strategy documents is needed. This examination provides a context for establishing the strategic need for cybersecurity defense responsibilities within the Federal government.

The first document created by the Federal government is the National Strategy for Homeland Security released in 2002. According to this strategy document, the U.S. government spent roughly $100 billion a year on homeland security prior to 2003, and this figure does not include additional funds provided to the armed forces for cybersecurity defense.[13] As such, this initial national security document was developed by the Department of Homeland Security (DHS) to address national safety interest in relation to both cyberspace and e-commerce. However, the purpose for incorporating cybersecurity into this document was the concern for protecting critical infrastructure within the public-private domain. To this end, this strategy briefly discusses critical infrastructure (CI) responsibilities as they pertain to DHS and what CI roles other government agencies may be tasked with. Specific DHS guidance regarding cybersecurity defense is exceptionally vague and Federal agency roles outside of lead CI protection assignments appear to be non-existent. The application of cybersecurity defense was very new in 2003 and the lack of expertise in this realm may have contributed to these omissions. This document does however make clear recommendations for physical actions that state, local government, private company, and American citizen can participate in to improve the material security of homeland CI

security. Specifically it identifies two national objectives of cybersecurity defense: cyber defense information sharing within the federal government and private industry; and integration of computer network security between state and local governments, and private industry. This strategy also directed multi-agency access to vast amounts of internal data residing within each of the Federal agencies.

The second U.S. cybersecurity defense document– the National Strategy for the Protection of Critical Infrastructures and Key Assets (2003) was developed in conjunction with the National Strategy for the DHS. This document provides specific leadership and administration roles for Federal government agencies and tasked with CI protection and establishes CI sectors for public-private partnerships. It assigns Federal agency leads for the eighteen CI sectors and directs these leads to maintain collaborative relationships with state, local government, and industry counterparts for each assigned area. It also directs the DHS to serve as the lead CI sector coordinator and primary liaison for cooperation among federal agencies, state governments, and private sectors regarding CI sector security.[14] The guidance contained in this document also recommends the expansion of voluntary cybersecurity-related information sharing between public-private organizations. This last policy guidance will become a future foundational activity for national cybersecurity defense.

The third cybersecurity defense document also released by the U.S. government in 2003 is the National Strategy to Secure Cyberspace. This strategic text is the first to concentrate on overall cybersecurity defense as its primary focus and recommends Federal leadership through a single government entity that helps detect, monitor, and analyze cyber attacks.[15] In this capacity, government leadership is directed to

consolidate federally funded cybersecurity research within the DHS to ensure strategic direction and improve public-private industry cyber defense. This includes three primary goals: prevention of cyber attacks against American CI; declining infrastructure susceptibility to cyber attacks; and decreasing the damage and recovery time from cyber attacks that do occur.[16] In order to translate each of these goals into accomplished cybersecurity defensive action, each target area is supplemented by five strategic actions. These include: the creation of a Cybersecurity response structure focused on cybersecurity incidents, developing a Cybersecurity Threat Reduction Program, creating a Cybersecurity Awareness Program, and establishing a system of National and Federal network security cooperation. In essence, the National Strategy to Secure Cyberspace encourages companies to routinely review their internal security plans and regularly add defensive technology based software protection to their network systems. However, cybersecurity of software updates during development and procurement has added another layer of concern to the cybersecurity defense supply-chain-management arena.

The Comprehensive National Cybersecurity Initiative (CNCI) released in 2008 is the fourth cybersecurity defense related document; although it is more of a policy text than an official strategy. This document is focused primarily on the need for cyber defense guidance from the Federal government. Introduced by President George W. Bush, the CNCI consists of consolidating mutually reinforcing cybersecurity initiatives that support his National Security Presidential Directive 54 and Homeland Security Presidential Directive 23 (NSPD-54/ HSPD-23).[17] This included accomplishing cybersecurity policies in a collaborative Federal agency atmosphere. The CNCI focused

on three initiatives: establishing front line defenses against cyber intrusions; by enhancing situational awareness of network vulnerabilities within Federal agencies; defend against full spectrum cyber threats; by enhancing counterintelligence capabilities and security for supplied technologies; and strengthening the future cybersecurity defense environment; by expanding cyber education and Federal agency efforts to deter malicious activity in cyberspace.[18] In building the CNCI plan, the government quickly realized that enabling national cybersecurity efforts required key foundational capabilities such as intelligence collection and law enforcement to support information assurance and cyber data processing and analysis functions. Furthermore, guidance to these organizations was explicit regarding protection of the civil liberties and privacy rights of American citizens.

Furthermore, in 2009 the Obama administration leaned forward to improve upon the CNCI measure by initiating a Cyberspace Policy Review that further examined existing cybersecurity strategies, policies, and procedures for transparency, consolidation, and intended effectiveness. This analysis resulted in a range of improved threat and vulnerability reduction recommendations, reinforced several CNCI incident response resiliency actions, and proposed recovery activities designed to protect U.S. network operations through information assurance.[19] The Cyberspace Policy Review concluded that improved information sharing across public-private organizations is a key component of effective cybersecurity defense. Additionally, it recommended that the three CNCI initiatives should be used as a base line to develop a streamlined, more up to date, unified national cybersecurity strategy. Specifically this new unified cybersecurity strategy must included the following enhanced cybersecurity programs:

clearly defined cybersecurity-related roles for the Federal government– to provide updated policies, authorities, and appropriate coordination for cybersecurity mission performance; establish Federal government partnerships within CI sectors– as cybersecurity public-private partnership need carefully defined relationships; implement universal methods for national network defense and or cyber attack responses; and issue a coordinated response process for Federal, State, local governments, and private businesses to any significant cybersecurity related incidents.[20]

In order to realize the near term objectives identified in the proposed unified cybersecurity defense strategy, the White House issued an updated National Security Strategy (NSS) in May 2010. It declares the American digital infrastructure as a strategic national asset, officially prioritizes cybersecurity threats as serious national security issues, and recognizes protection of the Internet and e-commerce as a primary concern. The NSS requires Federal agencies and private sectors responsible for cybersecurity defense to "deter, prevent, detect, defend against, and quickly recover from cyber intrusions and attacks.[21] This strategy also promotes development of cybersecurity network defense via resilient, secure systems, supported by cutting-edge technology and information assurance. Furthermore, in an effort to expand the coordinated Federal agency effort to establish a joint foundation for cybersecurity defense, the NSS relies on cybersecurity planning, resourcing, and awareness training to meet the desired end state.

In an effort to nest its cybersecurity defense strategy in support of the amalgamated effort expressed in the NSS, the Department of Defense's (DoD) Strategy for Operating in Cyberspace centers on defensive cybersecurity operations. This

document is concentrated on preventing potential U.S. adversaries from exploiting, disrupting, denying, and degrading the networks and systems that DoD depends on for normal operations.[22] In developing this operations focused strategy, the DoD identified its primary cyber risks as external actors, insider threats, and supply chain vulnerabilities.[23] In this manner, prevention methods for; "theft or exploitation of data; network disruption or denial of services; and the corruption, manipulation, or destructive actions that threaten to destroy and degrade network systems"[24] are discussed. In this capacity, DoD will treat cyberspace as an operational domain; employ new defense operating concepts in protecting network systems; build robust relationships and partner with other government agencies and private sectors; leverage national ingenuity through cyber workforce technological innovation."[25] Additionally, through this document, DoD encourages collective self-defense as a cornerstone for overall cybersecurity defense.

Although U.S. cybersecurity strategy documents have morphed from non-integrated manuscripts to cyber defense relevant policy guides over the last decade, the transformation of these strategic initiatives into holistic, universal cybersecurity defense actions has been difficult to achieve. For example in January 2008, President Bush directed the employment of CNCI proposals within the Departments of Homeland Security (DHS) and Defense in reaction to escalating cyber intrusions on government systems and Federal networks. In response the National Cyber Security Center (NCSC) was established within DHS to coordinate cyber security information sharing between these two departments and other federal agencies, improve overall federal agency collaboration, and shore up national network security.[26] However, these activities failed

to take hold because of several distressing factors. First, the President's guidance lacked formal, overall leadership to exercise legitimate authority and standardize implementation of cybersecurity protocols across Federal institutions. Second, leadership shortages that quickly developed within the NCSC in 2009 resulted in unstable defense management of government information networks. Lastly, as a consequence of meager leadership, most Federal agencies opted to pursue internal cybersecurity actions independently.

Similarly in 2010, after the United States Government Accountability Office (GAO) issued its report on all existing U.S. national cybersecurity (CS) policies,[27] President Obama established a Cybersecurity Coordinator as a Special Assistant to the White House, responsible for managing national cybersecurity defense efforts. The GAO review focused primarily on the identification of federal agency leads for strategic cybersecurity defense and illuminating cybersecurity defense responsibilities within these different government organizations. As such, it concluded that formal leadership across federal agencies regarding cybersecurity defense was almost non-existent, and a lack of clearly defined cybersecurity defense roles among Federal agencies was apparent.[28] To remedy these short comings through executive direction, the Cybersecurity Coordinator was tasked by the President to improve Federal agency collaboration and cybersecurity defense information sharing. However, this newly appointed national cyber defense official once more lacked any recognized command authority or budget control over the government agencies directed to lead. As in the previous example successfully influencing Federal organizations proved to be difficult, as the second Cybersecurity Coordinator–Michael Daniel, described in a statement just

after he took office in July 2012: “partnership with the private sector, completion of the National Level Cybersecurity Exercise, and the push for comprehensive cybersecurity legislation [are a few of the success stories of the current administrations cybersecurity defense actions]; however, much more engagement still needs to be accomplished to achieve universal cooperative action among the Federal departments.”[29] This becomes painfully evident as many government agencies in collaboration with the cyber coordinator still continue to report confusion and frustration as they attempt to employ lead and support roles in support of federal cybersecurity defense policies. So why is cybersecurity strategy so difficult to execute? A brief examination of critical federal agency roles in cybersecurity defense may provide some explanation.

According to the March 2010 GAO[30] report there are multiple federal agencies that have a substantial role in cybersecurity defense. These governmental organizations have been identified as the Executive Branch, the Department of Defense, the Department of Homeland Security, the Department of State, the Department of Justice, and the Department of Commerce. Each of these cabinet level organizations will be described in detail to identify their specific roles and responsibilities for providing national cybersecurity defense, to include any specialized supporting elements contained within them.

At the top of the federal agency hierarchy, the new Cybersecurity Coordinator is the lead official in the Executive Branch directly responsible for providing overall leadership for national cybersecurity defense. In this capacity, the cybersecurity coordinator serves as an active participant on the National Security and National Economic Council Staffs, to ensure U.S. cybersecurity defense strategies are

coordinated through other agencies for improving overall national cybersecurity defense.[31] The cybersecurity coordinator also plays an instrumental role in instituting dialogue between DHS, DoD, and various private CI sector organizations. However, as previously mentioned, this position lacks financial budget control or formal authority over any federal agency and collaboration is strictly voluntary.

As such, in the three years since the first cybersecurity coordinator was appointed, only two of the ten near-term cybersecurity defense actions recommended in the Cyberspace Policy Review (CRP),[32] have been completed. These accomplishments include: a DOD-DHS Memorandum of Agreement for cybersecurity leadership responsibilities regarding information sharing and synchronization of organizational cybersecurity defense efforts; and the development of a positive feedback mechanisms for voluntary cybersecurity information sharing between the government and CI sector leads. This latter item facilitated dialogue between the Critical Information Partnership Advisory Council (CIPAC) and the government, to capture private partner comments regarding CI legislation proposals included in the 2012 Cybersecurity Act.

Assisting the cybersecurity coordinator with cybersecurity policy, is the Information and Communications Infrastructure Interagency Policy Committee (ICI-IPC) and the Office of Management and Budget (OMB). ICI-IPC's leadership is nested within the Homeland Security Council (HSC) and National Security Council (NSC) and its primary function is information and communications infrastructure policy coordination.[33] Furthermore, according to Knitter,[34] the OMB assist influences cybersecurity defense via the Office of E-Government and Information Technology (E-Gov). The E-Government office provides "direction in the use of Internet-based technologies, making

it easier for citizens and businesses to interact with the Federal Government electronically."[35]

Outside of the White House, DoD is the primary department responsible for providing operational cybersecurity defense, although it is in a supporting command and control relationship with DHS. In accordance with a recently signed Memorandum of Agreement (MOA)[36] between DoD and DHS, the two agencies are closely partnered, with DHS providing the lead role regarding strategic American cybersecurity defense. The purpose of this 2010 agreement, signed by both cabinet directors, is increasing interdepartmental collaboration and clearly defining the roles and responsibilities of each organization.[37] Additionally, DoD established (USCYBERCOM) headquarters to assist with its cybersecurity defense mission. USCYBERCOM was specifically created to plan, coordinate, integrate, synchronize, and direct cybersecurity activities to defend DoD information networks. To ensure the United States maintains freedom of action in cyberspace, DoD activities also include conducting full-spectrum cyberspace operations such as computer network defense (CND), computer network exploitation (CNE), and computer network attack (CNA).[38] In this capacity, the institution functions within three operational lines to support cybersecurity defense: as it is responsible for management of IT networks via the DoD Global Information Grid;[39] prevents cyber attacks from occurring through defensive operations;[40] and performs offensive operations when required to defend critical network infrastructure.[41]

Moreover, the commander of USCYBERCOM has multiple authorities as this person is also the director of the National Security Agency (NSA) and the Chief of the Central Security Service (CSS). This consolidated management allows the leadership to

collaborate with all three organizations regarding the conduct of full spectrum defensive operations. It is important to note that potential offensive cyber operations are the exclusive responsibility of DoD and are not included in the MOA previously discussed. Some examples of offensive operations may include; cyber warfare (CW), offensive cyberspace operations (OCO), cyber operational preparation of the environment (C-OPE), and cyber mission assurance. To participate in these cyber defense activities, USCYBERCOM utilizes several subordinate military cyber elements from each of the primary services. These include the Army Forces Cyber Command (ARCYBER), the Navy's Tenth Fleet Cyber Command (FLTCYBERCOM), the Twenty-fourth Air Force (AFCYBER), and the Marine Forces Cyber Command (MARFORCYBER).

Although its limited capabilities to execute national cybersecurity defense operations make this organization heavily reliant on DoD, DHS is the lead federal agency mandated to defend all federal information technology (IT) infrastructure and data networks. This direction is provided by NSPD 54 and HSPD 23.[42] [43] As such, DHS is congressionally funded as the supported organization for national and federal network domain (.gov) defense. In this role, DHS is the prime agency within the Federal government that is responsible for administration and direct "coordination with the private sector to protect the nation's critical infrastructure."[44] DHS cybersecurity functions are maintained within the National Protection & Programs Undersecretary Directorate,[45] and this entity operates the National Cyber Security Division (NCSD). The NCSD is responsible for joint public-private efforts to secure the National cyber interest.[46] According to its structure, NCSD leads the National Cybersecurity and Communications Integration Center (NCCIC), which is a full time operations center

responsible for developing the federal, state, local government, and private sector common operating picture (COP) for cybersecurity.[47] Additionally, NCSD directs the United States Computer Emergency Readiness Team (US-CERT). The US-CERT is also a twenty-four hour functional organization that provides operational support for the NCSD. For example during a cyber emergency, US-CERT provides response assistance, affords cyber attack protection for government domains, and facilitates information sharing/collaboration with state, local governments, and CI industry partners.[48]

Moreover, DHS via its NCSD sub-directorate will lead the National Cyber Response Coordination Group, which is tasked with providing a coordinated and synchronized government response during a significant national cyber event.[49] DHS also created the Information Sharing and Analysis Center (ISAC) to build partnerships between it and organizations that are external to the federal government. The ISAC teams work within NCCIC in response to real cyber emergency incidents. Currently, there are two ISAC teams - the Multi-State (MS-ISAC) and the Information Technology (IT-ISAC) unit. The Multi-State team responds to state level cyber incidents only, and the Information Technology team focuses on private-sector cyber events. This cyber specialist's public-private partnership has been especially beneficial in the protection of Federal information networks. Another sub-directorate of DHS responsible for cybersecurity is the U.S. Secret Service (USSS) agency. This organization is accountable for enforcing cybersecurity defense regulations and laws within all U.S. territories. Some of these actions include, but are not limited to; reducing financial losses through computer crime and identity theft investigations.

Consequently, the Department of Justice (DoJ) is another federal agency that is responsible for cybersecurity defense regulations and laws.[50] As such, the Federal Bureau of Investigations (FBI) has primary responsibility within DoJ to investigate and prosecute agencies, private organizations, and individuals that breach cybersecurity defense statutes. In this manner, the FBI oversees the National Cyber Investigative Joint Task Force (NCIJTF)[51] in support of strategic cybersecurity defense efforts. As a result, this cyber investigation unit performs as a multi-agency focal point for coordination, integration, and sharing of applicable information relevant to cyber threat inquiries.

Realizing the importance of federal cybersecurity defense, the Department of State (DoS) has also assumed a lead role in the nation's efforts to enhance international cyberspace security and cooperation.[52] As the lead federal agency responsible for American foreign affairs, DoS has a significant role in overseeing the implementation of global information policies related to cybersecurity defense, granted by its authority under the 2003 National Strategy to Secure Cyberspace. To realize this mission, several of State Department's bureaus, such as the Office of Cyber Affairs and the Bureau of Intelligence and Research (INR) are directed to assist with international cybersecurity cooperation. These two directorates are in charge of providing intelligence analysis and coordination across Federal agencies to support international outreach efforts in conjunction with cybersecurity defense[53]

Finally, the Department of Commerce (DoC) plays a significant role in cybersecurity defense as this agency is responsible for the administration of cyber-systems critical information technology infrastructure design. DoC has two important

divisions concerned with computer network security– the National Institute of Standards and Technology (NIST), responsible for providing Research & Development and Engineering support; and the National Telecommunications and Information Administration (NTIA) element– that is responsible for building, testing, monitoring, and measuring new information related technology principles,…for commercial and government entities.[54] NTIA programs are largely focused on significant features of the Internet cybersecurity system, such as online privacy and the free flow of information.[55] NTIA also provides support to the White House, by advising the President on matters pertaining to information and telecommunication policies.

Conclusion

As cybersecurity defense strategies impose greater structure across U.S. Federal agencies, the lack of unity of effort amplified by insufficient Federal leadership will continue to strain government cooperation within cybersecurity defense policy employment, information sharing, and cybersecurity regulations enforcement. Moreover, as the Federal network system continues to grow in size and agency use, the number of manifest vulnerabilities posed by cybersecurity threats will increase substantially. This growing menace to national and federal infrastructure requires a responsive coherent approach to cybersecurity defense that is capable of providing strategic leadership that is based upon a revitalized, coherent, comprehensive stand alone cybersecurity defense strategy.[56] To this end, increasing the U.S. cybersecurity defense posture must be achieved through public-private partnerships that incentivize the Federal government and private sector companies to share additional information and move away from the one way communication processes currently being utilized. In other words, cybersecurity defense coalitions between the federal government and the business

community need to evolve into a bi-lateral shared activity across all Federal agencies. As a joint team, government and private businesses can effectively reverse the dangerous trend established by closed agency processes and limited information exchanges. As such, information sharing programs in CI industries such as the Defense Industrial Base have been developed to minimize partnership barriers and facilitate public-private collaborations that ward off dangerous threats to critical information systems. This includes such actions as expanding the overall number of companies participating in cybersecurity incident information sharing, adding new platforms for participation in public-private cyber defense information sharing actions, and increasing collaboration by both parties to include real time identification of potential threats and immediate responses to cyber intrusions as they occur.[57]

In this capacity, the Federal government has made an effort to initiate improved data sharing actions through efforts such as the data exchange initiative included in the 2009 DHS National Infrastructure Protection Plan and the Obama administration's CPR near-term follow up actions. Both documents suggest that improved government and private sector coalitions are a preliminary action to adequately enhance the protection of sensitive national information networks. However, guidance regarding exactly how to establish these partnerships is ambiguous and the responsibilities delineated for each of the partners appears to be in contradiction. For example, the CPR report asserts the Federal government is responsible for defending privately owned national infrastructure, but it also maintains that private industry retains autonomy for defending its critical systems. This lack of clarity regarding public-private cybersecurity partnership roles has resulted in the majority of the private-sector network operators assuming exclusive

responsibility for maintaining and defending their internal networks. To mitigate this single cybersecurity protection weak point, DoD adopted five key strategic initiatives, which included increasing its efforts to build stronger partnerships with CI private sector business as part of its 2011 Strategy for Operating in Cyberspace. This team oriented document appears to be well received by private industry, as several organizations representing the defense industrial base sector have indicated a desire to participate in a corporative public-private alliance framework, with a primary focus on increasing mutual cybersecurity network defense. Hence, the Defense Department created a cyber incident information sharing model known as the Defense Industrial Base (DIB) pilot in order to achieve a mutually desirable cybersecurity defense partnership program. This pilot is designed to improve cybersecurity defense by establishing mechanisms for voluntary cybersecurity information sharing between the Federal government and eligible DIB private organizations. Furthermore, the DIB model was also employed to enhance the comprehensive and preemptive defense capabilities of private organizations responsible for safeguarding unclassified DoD information. At the core of this cybersecurity defense program is the bilateral information sharing agreement in which the Defense Department provides cyber threat information, best practice recommendations, and information assurance support to DIB members; and in return for this information, DIB company participants report specified types of cyber intrusions to a centralized DoD threat information sharing and incident response unit known as the Defense Cyber Crime Center.

Advantages of the DIB partnership model are threefold; increased prioritization of cybersecurity efforts, cost reduction by removal of redundant activity, and improved

delineation of responsibilities. However, the DIB process also has a significant flaw, as it has been difficult to implement this program in practice because free communication between public-private partners in the current setting is problematic. For example, the government has limited the amount of potential cyber attack information it provides to the private industry sectors for fear of compromising national secrets; and private industry is often reluctant to report successful cyber intrusion attacks for fear of future second and third order effects to the company's bottom line. Communication misunderstandings such as these can significantly hinder full participation in cooperative cybersecurity relationships and prevent the ability of the federal government to adequately protect sensitive information. This in turn diminishes the benefits of privileged government research and compromises the technical advantages of DoD operating systems.

Moreover, the holistic implementation of an innovative public-private cybersecurity team dynamic across Federal agencies requires congressional buy in to expand the program. The unfortunate reality is, however, that the Executive Branch, the House of Representatives, and some Republican senators are in disagreement regarding new legislation that allows multiple Federal agencies and critical sector organizations to exchange cyber defense information.[58] Disagreement exists because the White House contends that current cyber intelligence sharing processes do not contain enough personal privacy protections and security regulation protocols for private industry. Conversely, Congress maintains that the government should not be regulating private company security practices that make the process of cyber defense too restrictive.[59] While both positions are sound, the obvious objections– lack of trust

between parties, current laws and regulations that hinder complete information disclosure, and turf wars within the Federal government must be moderated in order to establish productive public-private collaborations. It is clear that information sharing is important, but it is not enough. New cybersecurity laws for public-private engagement that facilitate cybersecurity defense are also required.

To this end, lawmakers need to develop and institute a relevant, unified, comprehensive cybersecurity bill for the immediate protection of cyberspace such as the laws proposed in the National Asset Act of 2010 and again in the National Cybersecurity Act of 2012. Both of these documents provide the president the authority to institute protection measures for telecommunications networks, the electric grid, and financial support systems.[60] Moreover, the 2012 Cybersecurity Act also grants the Federal government the authority to conduct a top-level assessment of cybersecurity risks of sector-by-sector critical infrastructure, establish critical infrastructure designation procedures, develop risk-based cybersecurity performance requirements, implement cyber response and restoration plans, and provide requirements for securing critical infrastructure that includes notification of cyber risks and threats obligations.[61]

Unfortunately, both bills did not pass Congressional scrutiny as a fundamental disagreement over the proposed increase in government cybersecurity sponsored protocols and a need for minimal infringement upon private civil liberties exist. For example, although the authorities proposed in the 2010 legislation limited presidential actions to a thirty day period in the event of a national emergency only, skeptics still had concerns as this legislation also supported a controversial national internet shut down measure, which roused public sensitivity to greater government influence over networks

utilized and maintained by the private sector. Not surprisingly, many private sector tech industry cybersecurity support businesses would rather see cybersecurity defense actions incorporated through incentives, rather than new laws or regulations. The concern is new government laws may replace current practice with a system that is reliant on Federal mandates and this change could undermine efforts to achieve long-term success.[62] This point of view was recently demonstrated by an association of IT industry groups, which included the Center for Democracy and Technology, the Internet Security Alliance, and U.S. Chamber of Commerce, among others. Although this association's position may be desirable by a few organizations, it is also easily negated by a realistic approach to cybersecurity legislation that relies on bilateral accords for overall cybersecurity defense. The development of a unified cybersecurity data sharing process between the White House, its Federal agencies, and their supporting private CI sectors can provide advantages in improving real time communication of cyber intrusions and make or break U.S. efforts to develop a more robust computing infrastructure. New cybersecurity defense legislation that supports these efforts is an important first steps in improving the overall posture of cybersecurity defense, but how we choose to implement these new tools in the future is a critical.

Cyber intrusions on U.S. federal networks and unclassified data systems represent an unacceptable national risk for compromised information. As today's cyber intruders continue to penetrate American IT information systems and networks, the need to protect these systems has become a vital U.S. security interest. However, a lack of unity of effort in managing American cybersecurity defense issues is quickly evolving to critical levels. The Federal government has been entrusted with the

responsibility to protect and defend the country against all threats, including cyber defense. As such, all federal agencies have the duty to ensure the safety and wellbeing of American citizens using or conducting business on global network systems. The private sector, however, designs, builds, owns, and operates most of the digital infrastructures that America depends on, so federal protection must be provided in a collaborative manner with the support of these companies. Achieving sufficient cybersecurity defense in America's future requires individual, private, public, state, and federal cooperation to educate society, share information, promote security standards, and establish protocols to offensively and defensively investigate cyber intrusions.[63]

Beginning in 2003, the Federal government launched one initiative after another to protect critical U.S. infrastructure systems in a closed loop fashion that was specific to each agency's immediate needs. Over the past decade this practice has resulted in multiple cybersecurity protocols that limit information sharing between federal departments and public-private organizations. However, in an effort to mitigate this behavior, the Federal government now understands that closer relationships and data exchanges between cybersecurity defense leaders, government agencies and the private businesses that support them can lead to increased cybersecurity threat awareness and quicker responses to cyber intrusions. Therefore, any U.S. strategic vision for cybersecurity defense needs to be holistic in its approach to effectively confront the lack of federal cybersecurity leadership and information sharing. The President's Cybersecurity Coordinator is a step in the right direction to provide comprehensive federal leadership; however, America's cybersecurity defense cannot simply be solved by the appointment of a senior government official. This is clearly

highlighted in the 2010 GAO assessment of the Federal government's poor cybersecurity defense structure and its inability to effectively address the growing problem of cybersecurity threats.[64] If the Cybersecurity Coordinator is going to be successful in leading federal efforts for cybersecurity defense, this individual also needs effective and binding legislation to build a cohesive national government that espouses cybersecurity defense capabilities devoid of Federal agency "rice bowls," more aligned with America's national security interests.[65] In this regard, the U.S. needs to create policies and processes through government leadership that focuses on the development of technologies and shared programs that mitigate cybersecurity risks.[66] As such, the Executive Branch's cybersecurity leadership requires the authoritative power that allows the newly appointed Cyber Coordinator to guide and motivate a collaborative, better equipped cybersecurity defense element. For example, Harknett and Stever,[67] posit the importance of a balanced commitment between the Government and its residents cannot be over emphasized, as the national objective to secure cyber defense cannot be achieved without engagement with all agencies and citizens. To meet sustained U.S. cybersecurity defense objectives utilizing immediate resources on hand, a marginal realignment of the current cybersecurity organizational structure, supported by updated legislation is necessary. These minor modifications provide the opportunity for the Federal government to expand its leadership role, improve interagency and private sector collaboration, develop oversight criteria for cybersecurity defense, and bolster America's cybersecurity defense position. However, a comprehensive cybersecurity defense strategy is also required to garner support from Congress and the public at large, in order to move towards this desired end state. As such, Federal agencies and

Congress, working with key private stakeholders need to embrace an effective common operating picture that supports universal cybersecurity strategy and defense, while simultaneously integrating information on the basis of informed and prioritized vulnerability mitigation. Our Nation's senior policymakers must think through the long-range strategic options available to the United States in a world that depends on assuring the use of cyberspace for its continued economic prosperity and national security. The time has come for the "government to commit the resources to build and nurture a highly skilled cyber workforce" capable of overcoming cyber threats and vulnerabilities.[68]

Endnotes

[1] President Barack A. Obama, "Speech: *Securing our Nation's Cyber Infrastructure",* 29 May 2009, linked from *The White House Home Page* at "Cybersecurity," http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure (accessed December 28, 2012).

[2] No Author Identified, "*The White House Home Page",* http://www.whitehouse.gov/cybersecurity (accessed December 28, 2012).

[3] President Obama, Speech: "*Securing our Nation's Cyber",* http://www.whitehouse.gov/the_press_office (accessed December 28, 2012).

[4] Internet Security Alliance, "The Cyber Security Social Contract: Policy Recommendations for the Obama Administration and 111th Congress", 5.

[5] Alexander Klimburg, "*National Cyber Security Framework Manual"*, (NATO CCD COE Publication, Tallinn 2012), xv.

[6] Ibid, 21-25.

[7] Ibid

[8] Ibid, 23.

[9] Ibid, xv.

[10] No Author Identified, "Department of Defense Dictionary of Military and Associated Terms," December, 15 2012, *linked from the PCMag Homepage* at

http://www.pcmag.com/encyclopedia_term/0,1237,t=DOD+intelligence+glossary&i=62536,00.asp or www.dtic.mil/doctrine/new_pubs/jp1_02.pdf (accessed December 10, 2012).

[11] U.S. Joint Chiefs of Staff, "Joint Communications System," Joint Publication 6-0. (Ft. Belvoir, VA: DTIC, 2010).

[12] U.S. Government Accountability Office (GAO), "Defense Department Cyber Efforts: More Detailed Guidance Needed to Ensure Military Services Develop Appropriate Cyberspace Capabilities," (Washington, DC: U.S. Government Accountability Office, 2011), 5.

[13] George W. Bush, *National Strategy for Homeland Security* (Washington, DC: The White House, July 2002), viii, xii.

[14] George W. Bush, *National Strategy for the Protection of Critical Infrastructures and Key Assets* (Washington, DC: The White House, July 2002), x.

[15] George W. Bush, *National Strategy to Secure Cyberspace* (Washington, DC: The White House, February 2003), viii.

[16] Ibid.

[17] George W. Bush, *Comprehensive National Cybersecurity Initiative CNCI* (Washington, DC: The White House, January 2008), 2-6.

[18] Ibid

[19] Barack A. Obama, *Cyberspace Policy Review* (Washington, DC: The White House, May 2009), iii-v.

[20] Ibid, iii-vi.

[21] Barack A. Obama, *National Security Strategy* (Washington, DC: The White House, May 2010), 27-28.

[22] Bill Gates, *Department of Defense Strategy for Operating in Cyberspace* (Washington, DC: Department of Defense, July 201), 2-4.

[23] Ibid

[24] Ibid

[25] Bill Gates, *Department of Defense Strategy for Operating in Cyberspace* (Washington, DC: Department of Defense, July 201), 5-10.

[26] David A. Powner, "Summary Cybersecurity: Progress Made but Challenges Remain in Defining and Coordinating the Comprehensive National Initiative," Government Accountability Office, no. GAO-10-338 (March 5, 2010): 1.

[27] Ibid.

[28] David A. Powner, "Summary Cybersecurity: Progress Made but Challenges Remain in Defining and Coordinating the Comprehensive National Initiative," Government Accountability Office, no. GAO-10-338 (March 5, 2010): 1.

[29] Michael Daniel, "Collaborative and Cross-Cutting Approaches to Cybersecurity," August 1, 2012, linked from *The White House Home Page* at "Cybersecurity", http://www.whitehouse.gov/cybersecurity (accessed December 28, 2012).

[30] U.S. Government Accountability Office (GAO), "Progress Made but Challenges Remain in Defining and Coordinating the Comprehensive National Imitative," (Washington, DC: U.S. Government Accountability Office, 2010), 1.

[31] President Barack A. Obama, "Speech: *Securing our Nation's Cyber Infrastructure",* 29 May 2009, linked from *The White House Home Page* at "Cybersecurity," http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure (accessed December 28, 2012).

[32] Barack A. Obama, *Cyberspace Policy Review* (Washington, DC: The White House, May 2009).

[33] Ibid

[34] Kelly T. Knitter, "Assessment of Cybersecurity Management", Strategy Research Project (Carlisle Barracks, PA: U.S. Army War College, March 22, 2012), 6.

[35] Office of Management and Budget (OMB), E-Gov Website at http://www.whitehouse.gov/omb/egov, (accessed December 28, 2012).

[36] No Author Identified, "Memorandum of Agreement between DHS and DoD Regarding Cybersecurity," September 2010.

[37] Ibid

[38] United States Strategic Command Website, U.S. CYBERCOM, at http://www.stratcom.mil/factsheets/cyber_command/, (accessed December 28, 2012).

[39] DOD Global Information Grid operations are actions taken to direct, and provide guidance and unity of effort to support efforts to design, build, configure, secure, operate, maintain, and sustain DOD networks to create and preserve availability, integrity, authentication, confidentiality and non-repudiation of information. U.S. Cyber Command, *USCYBERCOM Concept of Operations*, Version 1.0 (Sept. 21, 2010).

[40] Defensive cyberspace operations direct and synchronize actions to detect, analyze, counter, and mitigate cyber threats and vulnerabilities; to outmaneuver adversaries taking or about to take offensive actions; and to otherwise protect critical missions that enable U.S. freedom of action in cyberspace. This line of operation can trigger offensive cyberspace operations or other response actions necessary to defend DOD networks in response to hostile acts, or demonstrated hostile intent. U.S. Cyber Command, *USCYBERCOM Concept of Operations*, Version 1.0.

[41] Offensive cyberspace operations are the creation of various enabling and attack effects in cyberspace, to meet or support national and combatant commander's objectives and to actively defend DOD or other information networks, as directed. The primary U.S. Cyber Command offensive operational method will be effects-based operational planning and execution. U.S. Cyber Command, *USCYBERCOM Concept of Operations*, Version 1.0.

[42] George W. Bush, *National Security Presidential Directive 54: Cyber Security and Monitoring: Critical Infrastructure Identification, Prioritization, and Protection* (Washington, DC: The White House, January 2008).

[43] George W. Bush, *Homeland Security Presidential Directive 23: Cyber Security and Monitoring* (Washington, DC: The White House, January 2008).

[44] Department of Homeland Security Website, "Cybersecurity," at http://journal.dhs.gov/2009/06/focused-effort-on-cybersecurity.html, (accessed December 28, 2012).

[45] James A. Lewis and Katrina Timlin, "Cybersecurity and Cyberwarfare 2011: Preliminary Assessment of National Doctrine and Organization," UNIDIR Resources, 21.

[46] Department of Homeland Security Website, "National Cyber Security Division," at www.dhs.gov/xabout/structure/editorial_0839.shtm, (accessed December 28, 2012).

[47] Department of Homeland Security, "National Cybersecurity and Communications Integration Center (NCCIC) Website," at http://www.dhs.gov/files/programs/nccic.shtm, (accessed December 28, 2012).

[48] Department of Homeland Security, "United States Computer Emergency Readiness Team (US-CERT) Website," at http://www.us-cert.gov/aboutus.html, (accessed December 28, 2012).

[49] George W. Bush, *Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection* (Washington, DC: The White House, December 2003).

[50] Ibid, 23.

[51] Ibid

[52] David A. Powner, "Cyberspace – U.S. Faces Challenges in Addressing Global Cybersecurity and Governance," Government Accountability Office, no. GAO-10-606 (July 2010), 26.

[53] Ibid, 26.

[54] Department of Commerce, "National Institute of Standards and Technology Website," at http://www.nist.gov/index.html,(accessed 15 December 2012).

[55] Department of Commerce, National Telecommunications and Information Administration Website, http://www.ntia.doc.gov/,(accessed 15 December 2012).

[56] Powner, "Cyberspace – U.S. Faces Challenges" Government Accountability Office, no. GAO-10-606 (July 2010), 30.

[57] Erik Bataller, "Cyber Partnerships," Information Week, March 28, 2011, 21-24.

[58] Pam Benson, "Cyber security bill promotes sharing of threat data," CNN, November 30, 2012, linked from *The CNN Home Page* at http://security.blogs.cnn.com/2011/11/30/cyber-security-bill-promotes-sharing-of-threat-data, (accessed 12January 2012)

[59] Aliya Sternstein, "Network Defense," Government Executive 44 no. 7, (Jul 2012), 37.

[60] Ibid, 24-1-24.

[61] No Author Identified, "Library of Congress Summary: Cybersecurity Act of 2012," 112th Congress: Cybersecurity Act of 2012. (2012), linked from *The Library of Congress Home Page* at http://www.govtrack.us/congress/bills/112/s2105, **(accessed** January 10, 2013**).**

[62] Bataller, "Cyber Partnerships," 21-24

[63] Davi M. D'Agostino, "Defense Department Cyber Efforts, More Detailed Guidance Needed to Ensure Military Services Develop Appropriate Cyberspace Capabilities," Government Accountability Office, no. GAO-11-421 (May 2011), 3, or http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf, (accessed 15 December 2012).

[64] Ibid

[65] Ibid, 26.

[66] Cyberspace Policy Review, "Assuring a Trusted and Resilient Information and Communications Infrastructure," at http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf, (accessed 15 December 2012).

[67] Richard Harknett and James Stever, "The Cybersecurity Triad: Government, Private Sector Partners, and the Engaged Cybersecurity Citizen," University of Cincinnati Political Science Department.

[68] Max Stier, "Government Should Help Widen Cyber Knowledge," at http://www.federaltimes.com/article/20090914/ADOP06/909140302/1037/ADOP00,(accessed 15 December 2012).